SAND2020-7135C

The Center for Cyber Defenders

Expanding computer security knowledge

Reverse Engineering and Embedded Processor Analysis

Grant Brown, Tennessee Tech University; Matthew Gaydos, Purdue University;

Nicholas Wallace, Utah State University

Project Mentor: Josh Templin, 5638

Problem Statement:

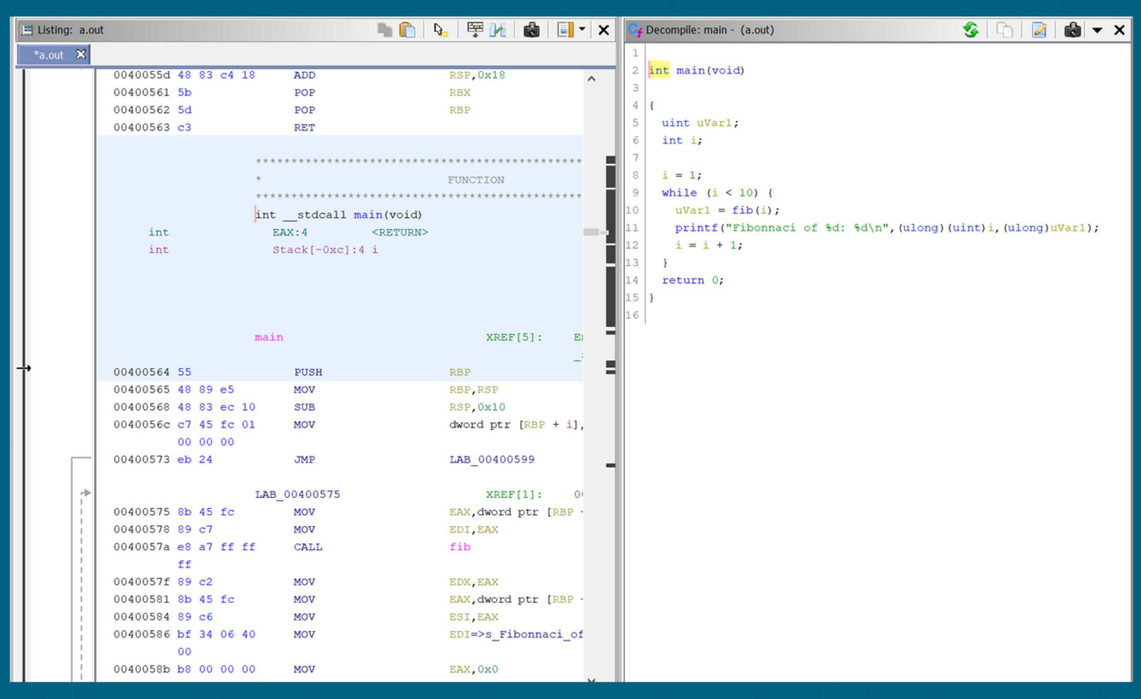
Ghidra is a powerful NSA-developed software reverse engineering tool. It’s capabilities are broad, such as the ability to reverse engineer firmware of all types, but are limited to those processor architectures which have been specified in Ghidra's database. Using Ghidra, we will answer project questions about specific firmware and processors. To do this, our tasks are reversing a firmware upgrade obfuscation algorithm, implementing a Ghidra processor specification by developing automation tools, and verifying this specification through Ghidra analysis scripts.

Objectives and Approach:

Task 1: Use Ghidra to Reverse Engineer a firmware upgrade obfuscation algorithm from a firmware binary.

Task 2: Improve Ghidra analysis by writing scripts that analyze and verify processor module implementations.

Task 3: Developing tools that automate SLEIGH processor module development for Ghidra.



Ghidra Disassembly of Example Program

Desired Results:

- Answer questions about desired firmware by creating an external tool that deobfuscates the firmware.
- Verify processor module implementations through improved Ghidra script analysis.
- Expanded Ghidra processor support through automated processor module development.

```
:mul^COND^SBIT_ZN rn,rm,rs  is $(AMODE) &  COND & c2527=0
& c2124=0 & SBIT_ZN & rn & c1215=0 & rs & c0407=9 & rm
{
  build COND;
  build rm;
  build rs;
  rn = rm*rs;
  resultflags(rn);
  build SBIT_ZN;
}
```

Example SLEIGH Definition of an Instruction

Impact and Benefits:

- Ghidra has extensive built-in functionalities but there exists a gap in Ghidra’s ability to decompile all files. This work will broaden Ghidra’s capabilities.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.